Preventing and Defending Against Cyber Attacks
October 2011

The Department of Homeland Security (DHS) is responsible for helping Federal Executive Branch civilian departments and agencies secure their unclassified networks (.gov). DHS also works with owners and operators of critical infrastructure and key resources (CIKR)—whether private sector, state, or municipality-owned—to bolster their cybersecurity preparedness, risk assessment and mitigation, and incident response capabilities.

The activities under way to implement the recommendations of the Cyberspace Policy Review build on the Comprehensive National Cybersecurity Initiative (CNCI) launched by President George W. Bush in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/ HSPD-23) in January 2008. President Obama determined that the CNCI and its associated activities should evolve to become key elements of a broader, updated national U.S. cybersecurity strategy. These CNCI initiatives will play a key role in supporting the achievement of many of the key recommendations of President Obama's Cyberspace Policy Review.

DHS has made significant strides to enhance the security of the nation's critical physical infrastructure as well as its cyber infrastructure and networks. Current tools include the National Cybersecurity Protection System, of which the EINSTEIN cyber intrusion detection system is a key component; the National Cybersecurity and Communications Integration Center, which serves as the nation's principal hub for organizing cyber response efforts; and a 2010 landmark agreement between DHS and the Department of Defense to align and enhance America's capabilities to protect against threats to critical civilian and military computer systems and networks.

Cybersecurity Coordination and Outreach

National Cyber Incident Response Plan

The President's Cybersecurity Policy Review called for *"a comprehensive framework to facilitate coordinated responses by Government, the private sector, and allies to a significant cyber incident."* DHS coordinated the interagency, state and local government, and private sector working group that developed the National Cyber Incident Response Plan.

The plan enables DHS to coordinate the response of multiple federal agencies, state and local governments, international partners, and private industry to incidents at all levels. It is designed to be flexible and adaptable to allow synchronization of response activities across jurisdictional lines.

In September 2010, the NCIRP was tested during the CyberStorm III national exercise, which simulated a large-scale attack on the nation's critical information infrastructure. Seven Cabinet agencies, eleven states, twelve international partners, and sixty private sector companies participated in the CyberStorm III exercise.

National Cybersecurity and Communications Integration Center (NCCIC)
In October 2009, DHS established the National Cybersecurity and Communications Integration Center, a 24-hour, DHS-led coordinated watch and warning center, to serve as the Nation's principal hub for organizing cyber response efforts and maintaining the national cyber and communications common operational picture.

- The NCCIC combines two of DHS's operational organizations: the U.S. Computer Emergency Readiness Team (US-CERT) and the National Coordinating Center for Telecommunications (NCC), the operational arm of the National Communications System.
- It also integrates the efforts of DHS's National Cybersecurity Center (NCSC), which coordinates operations among the six largest federal cyber centers, the DHS Office of Intelligence and Analysis and private sector partners.
- Additional representatives from federal agencies, the private sector and state and local governments are also collocated at the NCCIC including representatives from the energy sector, communications sector, and financial services sector.

U.S. Computer Emergency Readiness Team
DHS's U.S. Computer Emergency Readiness Team (US-CERT) is the operational arm of NCSD that provides response support and defense against cyber attacks for the Federal Civilian Executive Branch (.gov) networks as well as private sector partners, upon request. US-CERT also collaborates and shares information with state and local government, industry, and international partners to address cyber threats and develop effective security responses.

- In FY2011, US-CERT responded to more than 100,000 incident reports, and released more than 5,000 actionable cybersecurity alerts and information products.
- US-CERT continually provides vulnerability information to nearly 600,000 subscribers through the National Cyber Alert System.

Critical Infrastructure and Key Resources
DHS works to ensure the systems that support critical infrastructure and key resources (CIKR) – the essential functions that underpin American society – are protected from cyber threats.

- The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) provides onsite support to owners and operators of critical infrastructure for protection against and response to cyber threats, including incident response, forensic analysis, and site assessments. ICS-CERT also provides tools and training to increase stakeholder awareness of evolving threats to industrial control systems.
- In August 2009, DHS and the Information Technology Sector Coordinating Council (IT-SCC) released the IT Sector Baseline Risk Assessment (ITSRA) to identify and prioritize national-level risks to critical sector-wide IT functions while outlining strategies to mitigate those risks and enhance national and economic security.
    - The ITSRA validated the resiliency of key elements of IT sector infrastructure while providing a process by which public and private sector owners and operators can continually update their risk management programs.
    - The ITSRA links security measures to concrete data to provide a basis for meaningful infrastructure protection metrics.
    - Following up on the 2009 assessment, DHS and the IT-SCC have released a number of specific risk management strategy documents to mitigate those identified risks.

Cybersecurity Initiatives and Exercises

The EINSTEIN Program

The EINSTEIN system is designed to provide the U.S. Government with an early warning system for intrusions to Federal Executive Branch civilian networks, near real-time identification of malicious activity, and automated disruption of that malicious activity.

- EINSTEIN 1: The first iteration of the EINSTEIN system was developed in 2003 and automates the collection and analysis of computer network security information from participating agency and government networks to help analysts identify and combat malicious cyber activity that may threaten government network systems, data protection and communications infrastructure.
- EINSTEIN 2: The second phase of EINSTEIN, developed in 2008, incorporated intrusion detection capabilities into the original EINSTEIN system. DHS is currently deploying EINSTEIN 2 to federal executive branch civilian agencies and Networx Managed Trusted Internet Protocol Services (MTIPS) providers, private internet service providers that serve federal agencies, to assist them with protecting their computers, networks and information.
  - EINSTEIN 2 has now been deployed at 16 of 19 departments and agencies. Additionally, the four MTIPS providers currently provide service to 21 federal agencies.
  - In 2010, EINSTEIN 2 sensors registered 5.4 million "hits," an average of over 450,000 hits per month. A hit is an alert triggered by a predetermined intrusion detection signature that corresponds to a known threat.
- EINSTEIN 3: DHS is currently developing the third phase of the EINSTEIN system – an intrusion prevention capability which will provide DHS with the ability to automatically detect and disrupt malicious activity before harm is done to critical networks and systems.

Trusted Internet Connections Initiative

As part of the President's Comprehensive National Cybersecurity Initiative (CNCI), DHS works with the Office of Management and Budget (OMB) to reduce and consolidate the number of external connections to the Internet that federal agencies have to the Internet through the Trusted Internet Connections (TIC) initiative.

- This initiative reduces the number of potential threats to government networks and allows DHS to focus monitoring efforts on limited and known avenues through which Internet traffic must travel.
- DHS conducts onsite evaluations of department and agency progress toward implementing TIC goals.

National Strategy for Trusted Identities in Cyberspace

In July 2010, DHS supported the White House publication of a draft National Strategy for Trusted Identities in Cyberspace – which seeks to secure the identities of individuals, organizations, services and devices during online transactions, as well as the infrastructure supporting the transaction – fulfilling one of the near-term action items of the President's *Cyberspace Policy Review*. In April 2011, the White House released the final version of the National Strategy for Trusted Identities in Cyberspace.

- The Strategy supports the protection of privacy and civil liberties by enabling only the minimum necessary amount of personal information to be transferred in any particular transaction.
- Individuals will have a single credential to log into any website, which will provide greater security than passwords alone and offers increased protection of online anonymity.

Intergovernmental Partnerships

DHS works closely with its federal and state partners to protect government cyber networks.

- In December 2009, DHS initiated a first-of-its-kind federal-state cybersecurity partnership to deploy DHS's EINSTEIN 1 cybersecurity system to the state of Michigan's government networks. As part of the partnership with Michigan, DHS's U.S. Computer Emergency Readiness Team (US-CERT) identified possible abnormal activities on Michigan's networks and address threats to critical cyber infrastructure—strengthening defenses against cyber attacks and the overall resiliency of Michigan's networks and cyber resources.
- DHS and OMB work cooperatively with agencies across the federal government to coordinate the protection of the nation's federal information systems through compliance with the Federal Information Security Management Act of 2002.
- In October 2010, DHS and the Department of Defense (DoD) signed a memorandum of agreement that aligns and enhances America's capabilities to protect against threats to our critical civilian and military computer systems and networks, including deploying a DoD support team to the NCCIC to enhance the National Cyber Incident Response Plan and sending a full-time senior DHS leader and support team to DoD's National Security Agency.
    - The MOA increases collaboration and information sharing, furthers strategic planning, provides mutual support for cybersecurity capabilities and synchronizes operational mission activities.
- In May 2010, DHS, with Federal partners, helped launch the National Initiative for Cybersecurity Education (NICE) from the Comprehensive National Cybersecurity Initiative, extending the scope of cyber education beyond the federal workplace to include the public and students in kindergarten through post-graduate school. The goal of NICE is to establish an operational, sustainable and continually improving cybersecurity education program for the nation to promote the use of sound cyber practices that will enhance the nation's security. The National Institute of Standards and Technology (NIST) is leading the NICE initiative, comprised of over 20 federal departments and agencies, to ensure coordination, cooperation, focus, public engagement, technology transfer and sustainability.
- In November 2010, the Multi-State Information Sharing and Analysis Center (MS-ISAC) opened their Cyber Security Operations Center, a 24-hour watch and warning facility, which will both enhance situational awareness at the state and local level for the NCCIC and allow the federal government to quickly and efficiently provide critical cyber risk, vulnerability, and mitigation data to state and local governments.

Public-Private Partnerships and Information Sharing
Private industry owns and operates the vast majority of the nation's critical infrastructure and cyber networks. Consequently, the private sector plays an important role in cybersecurity, and DHS has initiated several pilot programs to promote public-private sector collaboration.

- In February 2010, DHS, the Department of Defense, and the FS-ISAC launched a pilot designed to help protect key critical networks and infrastructure within the Banking and Finance Sector by sharing actionable information. Based on knowledge gained from the pilot, DHS is expanding its information sharing and incident response coordination processes with other critical infrastructure sectors and leveraging capabilities from within DHS and across the response community.
- In June 2010, DHS implemented the Cybersecurity Partners Local Access Plan, which allows cleared owners and operators of CIKR, as well as state technology officials and law enforcement officials, to access secret-level cybersecurity information and video teleconference calls via local fusion centers.

Cyber Storm III
In September 2010, DHS hosted Cyber Storm III, a response exercise in which members of the cyber incident response community address the scenario of a coordinated cyber event in which the National Cyber Incident Response Plan is activated, testing the National Cybersecurity and Communications Integration Center and the federal government's suite of cybersecurity response capabilities.

Promoting Public Awareness of Cybersecurity
DHS is committed to developing innovative new ways to enhance public awareness about the importance of safeguarding America's computer systems and cyber networks from attacks.

- Every October, DHS and its public and private sector partners promote efforts to educate citizens about guarding against cyber threats as part of National Cyber Security Awareness Month.
- In March 2010, Secretary Napolitano launched the National Cybersecurity Awareness Challenge — which called on members of the public and private sector companies to develop creative and innovative ways to enhance awareness of the importance of cybersecurity and safeguard America's computer systems and networks from attacks.
- In July 2010, seven of the more than 80 proposals were selected and recognized at a White House ceremony. The winning proposals helped inform the National Cybersecurity Awareness Campaign***, Stop. Think. Connect.***

***Stop. Think. Connect.* National Cybersecurity Awareness Campaign**
In October 2010, in conjunction with National Cybersecurity Awareness Month, DHS launched the ***Stop. Think. Connect.*** cybersecurity awareness campaign—a national public education campaign designed to increase public understanding of cyber threats and how individual citizens can develop safer cyber habits that will help make networks more secure. The campaign fulfills a key element of President Obama's 2009 Cyberspace Policy Review, which tasked DHS with developing a public awareness campaign to inform Americans about ways to use technology safely.

In June 2011, ***Stop.Think.Connect.*** identified three public service announcements from a national competition that inform Internet users of the importance of safe online practices. The campaign also upgraded its web presence including enhancements for outreach and increased efforts for community involvement, building on the Secretary's message that homeland security is a shared responsibility and requires everyone's participation.

Cybersecurity Workforce Development

DHS is focused on building a world-class cybersecurity team by hiring a diverse group of cybersecurity professionals—computer engineers, scientists, and analysts—to secure the nation's digital assets and protect against cyber threats to our critical infrastructure and key resources.

- The DHS National Cyber Security Division (NCSD) is hiring cybersecurity and information technology professionals, nearly tripling its cybersecurity workforce in FY 2009 and nearly doubling that number in FY 2010. NCSD currently has more than 260 cybersecurity professionals on board, with dozens more in the hiring pipeline.
- DHS and the National Security Agency co-sponsor the Centers of Academic Excellence in Information Assurance Education and Research programs, the goal of which are to produce a growing number of professionals with information assurance expertise in various disciplines. Currently, there are more than 140 colleges and universities that have been designated as Centers of Academic Excellence in Information Assurance Education and Research.
- DHS and the Department of State co-hosted Operation Cyber Threat (OCT1.0), the first in a series of Government-wide experiential and interactive cybersecurity training pilots designed to apply learning concepts and share best practices in a secure, simulated environment to build capacity within the federal workforce.
- In December 2010, the Institute of Electrical and Electronics Engineers (IEEE) Computer Society, the world's leading organization of computing professionals, formally recognized the Master of Software Assurance (MSwA) Reference Curriculum, which DHS sponsored through its Software Assurance (SwA) Curriculum Project.
  - The MSwA program is the first such curriculum of its kind to focus on assuring the functionality, dependability, and security of software and systems.
- DHS co-sponsored the annual Colloquium for Information Systems Security Education and the Scholarship for Services (SFS) Job Fair/Symposium, which brought together 55 federal agencies and more than 200 SFS students.

Privacy and Civil Liberties

DHS is committed to supporting the public's privacy, civil rights, and civil liberties. Accordingly, the Department has implemented strong privacy and civil rights and civil liberties standards into all its cybersecurity programs and initiatives from the outset.

- DHS established an Oversight and Compliance Officer within the National Protection and Programs Directorate (NPPD).
- Key personnel receive specific training on the protection of privacy and other civil liberties as they relate to computer network security activities.
- In an effort to increase transparency, DHS has published on its Web site, www.dhs.gov, privacy impact assessments of its entire EINSTEIN program.